



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of **Michael A. Epstein**
Serial No.: **08/994,878**
Filed: **12/19/97**
Title: **ADMINISTRATION AND UTILIZATION OF PRIVATE KEYS IN A
NETWORKED ENVIRONMENT**

Atty. Docket No.: **PHA 23-313**
Group Art Unit: **2766**
Examiner: **Ho S. Song**

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

RECEIVED

JAN 29 2002

Technology Center 2100

Sir:

Enclosed is an original plus two copies of an Appeal Brief in the above-identified application.

☒ A check in the amount of **\$310** is enclosed.

☐ The Commissioner has already been authorized to charge fees in this application to Deposit Account .

☐ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account _____. Enclosed is a copy of this sheet.

Respectfully submitted,

Robert M. McDermott, Esq.

Reg. No. 41,508

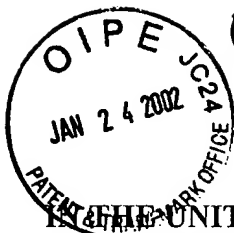
804-493-0707

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the
United States Postal Service as first-class mail in an envelope addressed to:
COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

On 22 October 2001

By



#15
1003

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of **Michael A. Epstein**
Serial No.: **08/994,878**
Filed: **12/19/97**
Title: **ADMINISTRATION AND UTILIZATION OF PRIVATE KEYS IN A
NETWORKED ENVIRONMENT**

Atty. Docket No.: **PHA 23-313**
Group Art Unit: **2766**
Examiner: **Ho S. Song**

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. § 1.192

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

RECEIVED
JAN 29 2002
Technology Center 2100

Sir:

This is an appeal from the decision of the Examiner dated 23 May 2001, finally rejecting claims 1, 2, 5-8, 11-16, and 19 of the subject application.

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to Philips Electronics North America Corporation, a company organized under the laws of the State of Delaware.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 2, 5-8, 11-16, and 19-20 are pending in the application. Claims 1, 2, 5-8, 11-16, and 19 stand rejected by the Examiner under 35 U.S.C. 103(a), and claim 20 is objected to by the Examiner, because it is dependent upon a cancelled claim. Claim 20 is cancelled in a concurrent amendment.

IV. STATUS OF AMENDMENTS

An amendment, canceling claim 20, is concurrently filed with this brief. No other amendments have been filed subsequent to the final rejection in the Office Action dated 23 May 2001.

V. SUMMARY OF THE INVENTION

The invention comprises a method and system for the administration and control of private keys of users within a network of communicating devices, or terminals.

Conventionally, each terminal on a network is associated with a particular user. The user, for example, has a personal computer (PC) at his or her workplace that is coupled to the network, and may or may not have a personal digital assistant (PDA) device, or other portable communicating device, that is also coupled to the network.

Private encryption keys are used to encrypt documents, or to digitally sign documents. A public key that corresponds to a user's private key, in a public-private key pair arrangement, is used to decrypt the encrypted documents, or to verify the user's digital signature. Generally, each key is a large, multi-byte, random number. A user is not expected to memorize the large random number corresponding to his or her private key; rather, the private key is stored in a file at each of the user's terminal. To prevent unauthorized access to the user's key, a password protection scheme is commonly used to limit access to the user's terminal, or to limit access to the user's key. Once a user securely logs into a terminal and network, conventional systems generally assume that the terminal is controlled by the user until the user logs out, or until a time limit is expired.

The paradigm of a terminal that is associated with a user, however, becomes inappropriate as networked terminals become ubiquitous. In an office environment, for example, a user may have a PC terminal and a telephone at his or her workspace. In a public area, such as a conference room, cafeteria, laboratory, and so on, the user will commonly place or receive telephone call using any available telephone instrument in the user's vicinity. In like manner, users in networked systems can be expected to routinely use networked terminals based on their proximity to the user, rather than based on their possession by the user. In this environment, the assumption that the user's private key

will be located at the user's terminal no longer holds true, and the assumption that the user is in control of the terminal until the user logs out relies heavily on the conscientiousness of the user to effect a proper log-out.

This invention provides a particularly effective and efficient method for administering and controlling users' private keys in a networked environment, wherein private keys are not retained at users' terminals, but are communicated to the terminal on demand from a server (Applicant's specification, page 3, line 28 through page 4, line 1). In accordance with the principles of this invention, an encrypted form of each user's private key is stored at a server facility (Applicants' specification, page 4, lines 2-8). When the user requires the private key, the user communicates an ID to the server, from any terminal on the network, and the server communicates the encrypted private key to the terminal. The user decrypts the private key at the terminal, based on a highly secure decryption key, or user identifying key, such as biometric information associated with the user, or a multi-word pass phrase (Applicant's specification, page 4, lines 15-25, and page 9, lines 2-18). The decrypted private key is then used to encrypt information, such as a hash of a document, constituting a digital signing of the document (Applicant's specification, page 5, lines 13-26). Upon completion of the encryption, the private key is deleted from the terminal (Applicant's specification, page 13, line 24 through page 14, line 1).

To assure that the user is actually present at the terminal when a given document is submitted for transmission, the server of this invention transmits the user's encrypted private key to the terminal, then validates the document only if the document is digitally signed using the decrypted private key. In combination with a terminal that is configured to delete the user's private key after each use, this process assures the presence of the user at the terminal when the document is signed.

Because the private keys are stored at the server in encrypted form, using an encryption that is personal to each user, the security of the technique of this invention is not vulnerable to an attack by someone who has access to the server system (Applicant's specification, page 4, lines 25-31). Even if the person has authorized access to the server system, security is maintained, because the information needed to decrypt each key is not stored at the server, nor at the network terminals. Because the decrypted private key is

deleted after each use, the technique of this invention is particularly well suited for a network of terminals that are accessible by a variety of users.

VI. ISSUES

Is claim 5 patentable under 35 U.S.C. 103(a) over Trostle (USP 5,919,257)?

Are claims 6-8 patentable under 35 U.S.C. 103(a) over Trostle in view of Schneier ("Applied Cryptography")?

Are claims 1, 11, 13, and 15 patentable under 35 U.S.C. 103(a) over Trostle in view of Spies (USP 5,689,565)?

Are claims 2, 6, 12, 14, 16, and 19 patentable under 35 U.S.C. 103(a) over Trostle in view of Spies and further in view of Schneier?

VII. GROUPING OF CLAIMS

Claims 1-2, 11-16, and 19 stand or fall together.

Claims 5-8 stand or fall together.

VIII. ARGUMENT

Claims 1-2, 11-16, and 19 address a method and system for administering private keys of a plurality of users. Claims 5-8 address a method for obtaining and using a private key at a user terminal, wherein the private key is deleted after use. Claims 1-2, 11-16, and 19 are separately patentable from claims 2-8, because claims 1-2, 11-16, and 19 include the storage and transmission of encrypted private keys, and the subsequent verification of a user's approval of a document, which is substantially independent of, and thereby novel and non-obvious over, a terminal that deletes private keys, as claimed in claims 5-8.

Is claim 5 patentable under 35 U.S.C. 103(a) over Trostle?

Trostle teaches a method and system for detecting whether an executable program at a user terminal, or workstation, has been illicitly changed (Trostle's Abstract). Trostle's process includes the transmission of an encrypted private key from a server to the workstation, and the decryption of the private key at the workstation, based on a user

password. The Examiner acknowledges that Trostle teaches the deletion of the user password from the workstation, but not the deletion of the private key.

In claim 5, the Applicant specifically claims the destruction, or avoidance of making a record, of the private key at the location of the user. The Examiner asserts that one of ordinary skill in the art would obviously modify Trostle to erase the private key as well as the user password, to reduce the chance of a hacker stealing data. The Applicant respectfully traverses this assertion, because Trostle specifically teaches the continued use of the private key after deleting the user password. Trostle teaches the use of a signature and random number to create a 'proof' that facilitates validating the authenticity of packets subsequently transmitted by the workstation to the network. This proof is encrypted using the decrypted private key and transmitted to the server, to validate the proof. (Trostle, page 6, lines 4-20). The Applicant respectfully maintains that Trostle's teachings are consistent with the conventional implicit association between a workstation and a user, in that, once the user successfully logs in, further user verification is unnecessary, and security items created during log-in are assumed to be valid, and secure, until the user logs out, or until a time limit is exceeded. Trostle's specific teaching of the use of the decrypted private key to validate the authenticity of transmitted packets to the network is contrary to the Examiner's assertion that one of ordinary skill in the art would obviously extend Trostle to eliminate the private key.

Because Trostle specifically teaches the use of the decrypted private key after deleting the user password, and claim 5 specifically teaches the destruction of the private key, the Applicant respectfully maintains that claim 5 is patentable under 35 U.S.C. 103(a) over Trostle.

Are claims 6-8 patentable under 35 U.S.C. 103(a) over Trostle in view of Schneier ?

The Examiner relies upon Schneier for teaching the use of a passphrase to encrypt the user's private key, and the Applicant concurs with this assessment of Schneier.

Claims 6-8 are dependent upon claim 5, which teaches the destruction of the user's private key. Because Trostle specifically teaches the use of the decrypted private key after deleting the user password, and claim 5 specifically teaches the destruction of the private key, the Applicant respectfully maintains that claims 6-8 are patentable under 35 U.S.C. 103(a) over Trostle in view of Schneier.

With further regard to claims 7 and 8, which specifically claim the use of the user's private key for signaling a user's approval of a document, as well as the destruction of the user's private key, the Examiner asserts that Trostle teaches receiving a digital signature that indicates a user's approval of a document (Referenced Office Action, page 3, third paragraph). The Applicant respectfully traverses this assertion, because Trostle is silent with regard to a user's approval, or disapproval, of a document.

The Examiner cites Trostle's FIG. 6 for teaching a user's approval of a document. Trostle's FIG. 6, however, merely illustrates a process for receiving a trusted hash value of one or more selected subprograms, and subsequently determining a computed hash value corresponding to these selected subprograms. Trostle's FIG. 6 does not reference a user input.

The Examiner also cites Trostle column 2, lines 44-60, for teaching a user's approval of a document. These referenced lines of Trostle specifically teach a process that verifies the integrity of executable programs, by comparing a trusted hash value of the program code to a currently determined hash value of the program code. If the program code has been modified, the current hash value will be different from the trusted hash value. This process is absolutely independent of a user's approval or disapproval, and is solely dependent upon the current hash value.

The Examiner also cites Trostle column 6, lines 10-25, for teaching a user's approval of a document. These referenced lines of Trostle teach the aforementioned validation of packets transmitted by the workstation, using a signature that is based on the user's private key and an authenticator credential. The authenticator credential and

signature is created when the user first enters the password that creates the decrypted private key. Column 6, lines 10-25 of Trostle is devoid of any mention of a user's approval:

Because Trostle neither teaches nor suggests the use of the user's private key for manifesting a user's approval of a document, with a subsequent deletion of the user's private key, as specifically claimed in claims 7 and 8, the Applicant respectfully maintains that claims 7 and 8 are patentable under 35 U.S.C. 103(a) over Trostle in view of Schneier.

Are claims 1, 11, 13, and 15 patentable under 35 U.S.C. 103(a) over Trostle in view of Spies?

Independent claims 1 and 11 specifically claim a method and system wherein an encrypted private key of a user is maintained at a storage that is remote from a user, and transmitting this encrypted private key to facilitate a verification of a user's approval of a document.

The Examiner asserts that Spies teaches the use of a private key to encrypt or decrypt a hash value, and the Applicant concurs with this assessment of Spies. The Examiner further asserts that it would be obvious to one of ordinary skill in the art to combine the teachings of Spies with Trostle to create the Applicant's invention. The Applicant respectfully traverses this assertion, because Trostle specifically teaches against involving a user in the verification process, and because Trostle employs the conventional association between a transmission from a user's terminal and the presence of the user.

Trostle teaches a system for verifying the integrity of a computer program at a user's workstation, and, as noted above, is silent with regard to securing a user's approval of a document. Trostle specifically notes that a "further *advantage* of the present invention is that it is *transparent to the user*."

The Applicant's invention is not transparent to the user, and is specifically designed to require an overt action on the part of the user to signal that the particular document is approved, rather than assuming that any document that is transmitted from a terminal at which the user logged-in is an approved document.

Trostle specifically teaches the creation of a proof-signature when the user logs into the network, and subsequently using this proof-signature "for *background* authentication and to further assist in *validating packets transmitted by the workstation*." Trostle's specific teachings of providing a process that is transparent to the user for validating transmissions from the workstation at which the user logged in is consistent with the conventional assumption that, once a user logs in at a terminal, transmissions from that terminal are assumed to be from that user, until the user logs out, or until a specified time-limit is exceeded. Trostle specifically teaches that the authenticator credential that is used to create the signature includes a duration of time that the authenticator is valid (Trostle, column 6, lines 7-11). When the network requests authentication of a transmitted packet, the *workstation* creates a proof, using the signature, the request, and a random number. The proof is then *encrypted by the workstation* using the user's decrypted private key (which the workstation *retained* after the user's initial login process). (Trostle, column 6, lines 13-22.) Trostle's process merely verifies that the packet was sent by the particular workstation that the user logged-in, within a given duration from the time that the user logged in. The user is not involved in any of this validation process, and anyone having access to this particular workstation can transmit anything during the authentication duration, independent of the user's approval. The workstation will continue to 'prove' that transmissions from the workstation came from the authorized user until the user logs out, or until the authentication duration expires.

The premise of the Applicant's invention is that the conventional association of a user's terminal to a presence of the user will become increasingly invalid as network terminals become ubiquitous. As such, the Applicant specifically teaches and claims a method and system that is suitable for an unassociated terminal-user relationship, and is designed to require the presence of the user to manifest the user's approval of a communicated document, rather than a terminal's verification that the document was transmitted by that particular terminal during a particular time period.

Because Trostle specifically teaches against involving a user who has logged into a system in a transmission verification process, and specifically reinforces the conventional assumption that all transmissions from a user's terminal are approved by the

user who logged into the system at that terminal, one of ordinary skill in the art would not be lead by Trostle or Spies to introduce an explicit user-approval process into Trostle's process. As such, the Applicant respectfully maintains that claims 1, 11, 13, and 15 are patentable under 35 U.S.C. 103(a) over Trostle in view of Spies.

Are claims 2, 6, 12, 14, 16, and 19 patentable under 35 U.S.C. 103(a) over Trostle in view of Spies and further in view of Schneier?

Claims 2, 6, 12, 14, 16, and 19 are dependent upon independent claims 1, 5, and 11, which are addressed above.

With regard to claim 6, which is dependent upon claim 5, Trostle does not teach the destruction of a user's private key, and specifically teaches the use of the user's private key to verify subsequent transmissions from the user's terminal.

With regard to claims 2, 12, 14, 16, and 19, which are dependent upon claims 1 and 11, Trostle does not teach securing a user's approval of a transmitted document, and specifically teaches against involving the user in the validation process, based on the conventional assumed correspondence between a transmission from a user terminal and a presence of the user.

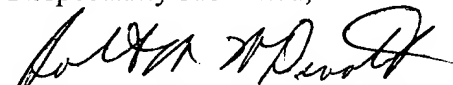
Based on the comments above, the Applicant respectfully maintains that claims 2, 6, 12, 14, 16, and 19 are patentable over Trostle in view of Spies and further in view of Schneier.

CONCLUSIONS

Because Trostle does not teach the destruction of a user's private key, and specifically teaches the use of the user's private key to verify subsequent transmissions from the user's terminal, the Applicant respectfully requests that the Examiner's rejection of claims 5-8 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Because Trostle does not teach securing a user's approval of a transmitted document, and specifically teaches against involving the user in the validation process, based on the conventional assumed correspondence between a transmission from a user terminal and a presence of the user, the Applicant respectfully requests that the Examiner's rejection of claims 1-2, 11-16, and 19 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,



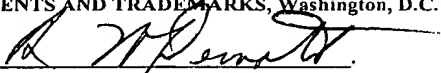
Robert M. McDermott, Attorney
Registration Number 41,508
804-493-0707

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

On 22 October 2001

By



APPENDIX

CLAIMS ON APPEAL

1. A method of administration of private keys for a plurality of users for use to encrypt or decrypt items transmitted via a network, there being for each user a respective set of an ID, user identifying information, private key, and public key corresponding to the private key, said method comprising:

receiving via the network a user's ID;

reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user;

sending via the network the encrypted private key, whereby the encrypted private key can be received and decrypted at the location of the user using the user's identifying information;

receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key; and

verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

2. The method of Claim 1, wherein the user identifying information comprises a passphrase entered by the user at the user equipment, or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

5. A method for obtaining and using a private key at user equipment via a network, said method comprising:

- transmitting from the user equipment an ID of a user;
- receiving a private key of the user encrypted with a user identifying key associated with the user; and
- decrypting the encrypted private key using a user identifying key determined from interaction with the user at the user equipment;
- using the decrypted private key; and
- destroying or avoiding making any non-volatile record of the private key at the location of the user.

6. The method of Claim 5, wherein

- the user identifying key determined by interaction with the user at the user equipment is determined from a passphrase entered by the user at the user equipment or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

7. A method as claimed in Claim 5, wherein the decrypted private key is used by:

- computing a hash of a document to manifest the user's approval of the document;
- encrypting the hash using the user's private key; and
- transmitting the encrypted hash.

8. A method as claimed in Claim 6, wherein the decrypted private key is used by:

- computing a hash of a document to manifest the user's approval of the document;
- encrypting the hash using the user's private key; and
- transmitting the encrypted hash.

11. A system for administering private keys and corresponding public keys for a plurality of users, comprising:

computer readable storage means and

a server,

characterized in that:

the storage means includes therein respective IDs and encrypted private keys for the respective users which private keys have been encrypted using respective keys determined from respective user identifying information, and

the server is configured:

to read an encrypted private key from the storage means associated with an ID corresponding to a particular user,

to transmit the encrypted private key to the particular user,

to receive a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key, and

to verify the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

12. The system of Claim 11, wherein the user identifying information comprises a passphrase or biometric information.

13. A system as claimed in Claim 11, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

14. A system as claimed in Claim 12, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

15. A system as claimed in Claim 11, characterized in that
the server is further configured
to decrypt data received from the particular user using the public key.
16. A system as claimed in Claim 12, characterized in that
the server is further configured
to decrypt data received from the particular user using the public key.
19. A system as claimed in Claim 16, further comprising
at least one user terminal interconnected via a network to the server,
characterized in that the user terminal is configured
for transmitting to the server via the network an ID entered by the user,
and
for receiving and decrypting an encrypted private key received via the
network from the server using a user identifying key determined from a passphrase
entered by the user or biometric information obtained by measuring the user.